CLAIMS

1. A prime calculating apparatus for calculating a prime candidate N larger than a known prime q and testing primality of the calculated prime candidate N, comprising:

an information storage unit storing the known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value;

a random number generation unit operable to generate a random number;

a candidate calculation unit operable to (i) read the prime q, the management information, and the verification value, (ii) calculate a multiplication value R by multiplying the management information by the random number, and (iii) calculate the prime candidate N, according to $N = 2 \times$ (multiplication value $R + w$) $\times$ prime $q + 1$, using w satisfying $2 \times w \times$ prime $q + 1$ = the verification value (*mod* the management information);

a primality testing unit operable to test primality of the calculated prime candidate N; and

an output unit operable to output the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined.

2. The prime calculating apparatus of Claim 1, wherein

the verification value stored in the information storage unit is 1, and

the candidate calculation unit calculates the prime candidate N according to $N = 2 \times$ multiplication value $R \times$ prime $q + 1$.

3. The prime calculating apparatus of Claim 1, wherein

the primality testing unit includes:

a 1st judging subunit operable to judge whether the prime candidate N satisfies $2^{N-1} = 1 \ mod \ N$; and

a 2nd judging subunit operable to perform, when the judgment of the 1st judging subunit is affirmative, one of judgments of (i) whether the prime candidate N and the multiplication value R satisfy $2^{2R} \neq 1 \ mod \ N$ and (ii) whether the prime candidate N and the multiplication value R satisfy $GCD(2^{2R}-1, N) = 1$, and to determine the primality of the prime candidate N when the performed one of judgments is affirmative.

4. The prime calculating apparatus of Claim 1, wherein

the information storage unit further stores a known prime g and a unique issue identifier, and

the prime calculating apparatus further comprising:

a prime generation unit operable to generate a prime gp by applying a prime generation function for generating a unique prime to the prime g and the issue identifier, and output the generated prime gp; and

a writing unit operable to write the generated prime gp to the information storage unit as the management information.

5. The prime calculating apparatus of Claim 4, wherein

the prime generation unit (i) generates a combination of the issue identifier and a variable c that is one of 0 and a positive integer,

(ii) calculates a prime candidate = $2 \times$ prime $g \times f$(the combination) + 1, and

(iii) tests primality of the calculated prime candidate, and outputs the calculated prime candidate as the prime gp when the primality of the calculated prime candidate is determined.

6. The prime calculating apparatus of Claim 5, wherein

when the primality of the calculated prime candidate is not determined, the prime generation unit (i) adds a value of 1 to the variable *c*,

(ii) generates a 2nd combination of the issue identifier and the variable *c* having the value of 1 added thereto,

(iii) calculates a 2nd prime candidate = 2 × prime *g* × *f*(the 2nd combination) + 1, and

(iv) tests primality of the 2nd calculated prime candidate, and outputs the 2nd calculated prime candidate as the prime *gp* when the primality of the 2nd calculated prime candidate is determined.

7. The prime calculating apparatus of Claim 1, further comprising:

an iteration control unit operable to control the random number generation unit, the candidate calculation unit, and the primality testing unit to iterate the random number generation, the calculation of the prime candidate *N*, and the primality testing, until the primality of the calculated prime candidate *N* is determined by the primality testing unit.

8. The prime calculating apparatus of Claim 7, further comprising:

a preparative prime storage unit storing a known prime *p*;

a preparative random number calculation unit operable to calculate a random number *R'*;

a preparative candidate calculation unit operable to calculate a prime candidate *N'*, according to *N'* = 2 × random number *R'* × prime *p* + 1, using the prime *p* and the calculated random number *R'*;

a preparative primality testing unit operable to test primality of the calculated prime candidate *N'*;

a preparative writing unit operable to write the calculated prime candidate N' to the information storage unit as a prime q when the primality of the calculated prime candidate N' is determined; and

a preparative iteration control unit operable to control the preparative random number calculation unit, the preparative candidate calculation unit, and the preparative primality testing unit to iterate the calculation of the random number R', the calculation of the prime candidate N', and the primality testing, until the primality of the calculated prime candidate N' is determined by the preparative primality testing unit.

9. The prime calculating apparatus of Claim 7 that is a key generating apparatus for generating a public key and a private key of RSA encryption, further comprising:

a public key generation unit operable to generate the public key using a calculated prime N; and

a private key generation unit operable to generate the private key using the generated public key.

10. The prime calculating apparatus of Claim 9, wherein

the public key generation unit (i) directs the iteration control unit to newly obtain a prime N', (ii) calculates a number n, according to n = prime $N \times$ prime N', using the prime N and the newly obtained prime N', and (iii) generates a random number e,

a combination of the calculated number n and the generated random number e is the public key,

the private key generation unit calculates d satisfying $e \times d = 1 \ mod \ L$,

L is a least common multiple of the prime $N - 1$ and the prime $N' - 1$,

and

the calculated d is the private key.

11. The prime calculating apparatus of Claim 9, wherein

the information storage unit further stores a different verification value from the verification value,

the public key generation unit directs the iteration control unit to newly obtain a prime N',

the candidate calculation unit calculates a prime candidate N', according to $N' = 2 \times$ multiplication value $R \times$ prime $q +$ the different verification value,

the public key generation unit calculates a number n, according to n = prime $N \times$ prime N', using the prime N and the newly obtained prime N', and generates a random number e,

a combination of the calculated number n and the generated random number e is the public key,

the private key generation unit calculates d satisfying $e \times d = 1 \ mod \ L$,

L is a least common multiple of the prime $N - 1$ and the prime $N' - 1$, and

the calculated d is the private key.

12. The prime calculating apparatus of Claim 9 that is a key issuing server apparatus for generating and issuing the public key and the private key of RSA encryption for a terminal, further comprising:

a key output unit operable to output the generated private key to the terminal; and

a publishing unit operable to publish the generated public key.

13. The prime calculating apparatus of Claim 12, further comprising:

an identifier obtaining unit operable to obtain a terminal identifier uniquely identifying the terminal;

a management information generation unit operable to generate the management information including the obtained terminal identifier; and

a writing unit operable to write the generated management information to the information storage unit.

14. The prime calculating apparatus of Claim 13, further comprising:

a server identifier storage unit prestoring a server identifier uniquely identifying the prime calculating apparatus functioning as the key issuing server apparatus, wherein

the management information generation unit further reads the server identifier from the server identifier storage unit, and generates the management information further including the read server identifier.

15. A prime verification apparatus for verifying the prime N output by a prime calculating apparatus of Claim 1, comprising:

a prime-verification-apparatus information storage unit storing the management information and the verification value;

a subtraction unit operable to obtain a prime subtraction value by subtracting the verification value from the prime N;

a judgment unit operable to judge whether the obtained prime subtraction value is divisible by the management information; and

a control unit operable to permit use of the prime N when the judgment

is affirmative, and prohibit the use of the prime N when the judgment is negative.

16. The prime verification apparatus of Claim 15, wherein

the prime calculating apparatus stores the verification value which is 1, and calculates a prime candidate N, according to $N = 2 \times$ multiplication value $R \times$ prime $q + 1$,

the verification value stored in the prime-verification-apparatus information storage unit is 1, and

the subtraction unit obtains the prime subtraction value by subtracting 1 from the prime N.

17. The prime verification apparatus of Claim 15, wherein

the prime calculating apparatus further (i) stores a known prime g and a unique issue identifier, (ii) generates a prime gp by applying a prime generation function for generating a unique prime using the prime g and the issue identifier, (iii) outputs the generated prime gp, and (iv) writes the generated prime gp to the information storage unit as the management information, and

the prime-verification-apparatus information storage unit further stores the prime g and the issue identifier, and

the prime verification apparatus further comprising:

a prime generation unit operable to generate the prime gp by applying the prime generation function for generating the unique prime using the prime g and the issue identifier, and output the generated prime gp; and

a writing unit operable to write the generated prime gp to the prime-verification-apparatus information storage unit as the

management information.

18. The prime verification apparatus of Claim 17, wherein

the prime calculating apparatus (i) generates a combination of the issue identifier and a variable *c* that is one of 0 and a positive integer, (ii) calculates a prime candidate = 2 × prime *g* × *f*(the combination) + 1, (iii) tests primality of the calculated prime candidate, and (iv) outputs the calculated prime candidate as the prime *gp* when the primality is determined, and

the prime generation unit (i) generates the combination of the issue identifier and the variable *c*,

(ii) calculates the prime candidate = 2 × prime *g* × *f*(the combination) + 1, and

(iii) tests primality of the calculated prime candidate, and outputs the calculated prime candidate as the prime *gp* when the primality is determined.

19. The prime verification apparatus of Claim 18, wherein

when the primality is not determined, the prime calculating apparatus (i) adds a value of 1 to the variable *c*, (ii) generates a 2nd combination of the issue identifier and the variable *c* having the value of 1 added thereto, (iii) calculates a prime candidate = 2 × prime *g* × *f*(the 2nd combination) + 1, and (iv) tests primality of the calculated prime candidate and outputs the calculated prime candidate as the prime *gp* when the primality of the calculated prime candidate is determined, and

when the primality of the generated prime candidate is not determined, the prime generation unit (i) adds the value of 1 to the variable *c*,

(ii) generates the 2nd combination of the issue identifier and the variable *c* having the value of 1 added thereto, and

(iii) tests primality of the calculated prime candidate and outputs the calculated prime candidate as the prime *gp* when the primality is determined.

20. The prime verification apparatus of Claim 15, wherein

the prime calculating apparatus is a key generating apparatus for generating a public key and a private key of RSA encryption, and further generates the public key of RSA encryption using the output prime *N* and generates the private key of RSA encryption using the generated public key, and

the prime verification apparatus is a key verification apparatus for verifying the public key, and

the prime verification apparatus further comprising:

an obtaining unit operable to obtain the public key; and

a verifying unit operable to verify validity of the obtained public key.

21. The prime verification apparatus of Claim 20, wherein

the prime calculating apparatus (i) newly obtains a prime N', (ii) calculates a number n, according to n = prime $N \times$ prime N', using the prime N and the newly obtained prime N', (iii) generates a random number e, and (iv) calculates d satisfying $e \times d = 1 \bmod L$, where L is a least common multiple of the prime $N - 1$ and the prime $N' - 1$, and a combination of the calculated number n and the generated random number e is the public key while the calculated d is the private key,

the obtaining unit obtains the combination of the number n and the random number e as the public key, and

the verifying unit includes:

a subtraction subunit operable to obtain a public-key subtraction value by subtracting a square value of the verification value from the obtained number n;

a judgment subunit operable to judge whether the obtained prime subtraction value is divisible by the management information; and

a control subunit operable to permit output of the public key when the judgment is affirmative, and prohibit the output of the public key when the judgment is negative.

22. The prime verification apparatus of Claim 20, wherein

the prime calculating apparatus further (i) stores a different verification value from the verification value, (ii) newly obtains a prime N' by calculating a prime candidate N', according to $N' = 2 \times$ multiplication value $R \times$ prime $q +$ the different verification value, (iii) calculates a number n, according to $n =$ prime $N \times$ prime N', using the prime N and the newly obtained prime N' and generates a random number e, and (iv) calculates d satisfying $e \times d = 1 \ mod \ L$, where L is a least common multiple of the prime $N - 1$ and the prime $N' - 1$, and a combination of the calculated number n and the generated random number e is the public key while the calculated d is the private key,

the prime-verification-apparatus information storage unit stores the different verification value,

the obtaining unit obtains the combination of the number n and the random number e as the public key, and

the verifying unit includes:

a subtraction subunit operable to obtain a multiplication value by multiplying the verification value and the different verification value and to obtain a public key subtraction value by subtracting the multiplication value from the obtained number n;

a judgment subunit operable to judge whether the obtained prime subtraction value is divisible by the management information; and

a control subunit operable to permit output of the public key when the judgment is affirmative, and prohibit the output of the public key when the judgment is negative.

23. The prime verification apparatus of Claim 20 that is a key verification server apparatus, wherein

the obtaining unit obtains, from a key issuing server apparatus for generating the public key and the private key of RSA encryption for a terminal, the public key.

24. The prime verification apparatus of Claim 23, wherein

the management information stored in the prime-verification-apparatus information storage unit includes a terminal identifier uniquely identifying the terminal, and

the judgment unit judges whether the obtained prime subtraction value is divisible by the management information including the terminal identifier.

25. The prime verification apparatus of Claim 24, wherein

the management information stored in the prime-verification-apparatus information storage unit includes a server identifier uniquely identifying the prime calculating apparatus functioning as the key issuing server apparatus, and

the judgment unit judges whether the obtained prime subtraction value is divisible by the management information including the server identifier.

26. The prime verification apparatus of Claim 23 that is a public-key-certificate issuing server apparatus, further comprising:

a certificate generation unit operable to generate, when the verifying unit determines that the public key is valid, signature data by applying a digital signature to public key information including at least the public key, and to generate a public key certificate including at least the signature data and the public key; and

a certificate output unit operable to output the generated public key certificate.

27. A key issuing system comprising a terminal and a key issuing server apparatus for generating and issuing a private key and a public key of RSA encryption for the terminal, wherein

the key issuing server apparatus includes:

an information storage unit storing a known prime q, management information corresponding to a prime to be generated, and a predetermined verification value;

a random number generation unit operable to generate a random number;

a candidate calculation unit operable to (i) read the prime q, the management information, and the verification value, (ii) calculate a multiplication value R by multiplying the management information by the random number, and (iii) calculate a prime candidate N, according to $N = 2 \times$ multiplication value $R \times$ prime $q +$ the verification value;

a primality testing unit operable to test primality of the calculated prime candidate N;

an output unit operable to output the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined;

an iteration control unit operable to control the random number generation unit, the candidate calculation unit, and the primality testing unit to iterate the random number generation, the calculation of the prime candidate N, and the primality testing, until the primality of the calculated prime candidate N is determined by the primality testing unit;

a public key generation unit operable to generate the public key of RSA encryption using an output prime N;

a private key generation unit operable to generate the private key of RSA encryption using the generated public key;

a key output unit operable to output the generated private key to the terminal; and

a publishing unit operable to publish the generated public key, and

the terminal obtains and stores the private key, and uses the stored private key.

28. The key issuing system of Claim 27, wherein

the key issuing server apparatus (i) newly obtains a prime N', (ii) calculates a number n, according to n = prime $N \times$ prime N', using the prime N and the newly obtained prime N' and generates a random number e, and (iii) calculates d satisfying $e \times d = 1 \ mod \ L$, where L is a least common multiple of the prime $N - 1$ and the prime $N' - 1$, and a combination of the calculated number n and the generated random number e is the public key while the calculated d is the private key, and

the key issuing system further comprising a key verification server apparatus which includes:

an obtaining unit operable to obtain the combination of the number n and the random number e as the public key; and

a verification unit operable to verify validity of the obtained public key, wherein

the verifying unit includes:

a subtraction subunit operable to obtain a public-key subtraction value by subtracting a square value of the verification value from the obtained number n;

a judgment subunit operable to judge whether the obtained prime subtraction value is divisible by the management information; and

a control subunit operable to permit output of the public key when the judgment is affirmative, and prohibit the output of the public key when the judgment is negative.

29. A prime calculation method used in a prime calculating apparatus that (i) includes an information storage unit storing a known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value, and (ii) calculates a prime candidate N larger than the known prime q and performs primality testing on the calculated prime candidate N, the prime calculation method comprising:

a random number generation step of generating a random number;

a candidate calculation step of (i) reading the prime q, the management information, and the verification value, (ii) calculating a multiplication value R by multiplying the management information by the random number, and (iii) calculating the prime candidate N, according to according to $N = 2 \times$ (multiplication value $R + w$) $\times$ prime $q + 1$, using w satisfying $2 \times w \times$ prime $q + 1 =$ the verification value (*mod* the management information);

a primality testing step of testing primality of the calculated prime

candidate N; and

an output step of outputting the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined.

30. A prime-calculation computer program used on a prime calculating apparatus that (i) includes an information storage unit storing a known prime q, management information that is an odd number and corresponds to a prime to be generated, and a predetermined verification value, and (ii) calculates a prime candidate N larger than the known prime q and performs primality testing on the calculated prime candidate N, the prime-calculation computer program comprising:

a random number generation step of generating a random number;

a candidate calculation step of (i) reading the prime q, the management information, and the verification value, (ii) calculating a multiplication value R by multiplying the management information by the random number, and (iii) calculating the prime candidate N, according to according to $N = 2 \times$ (multiplication value $R + w$) $\times$ prime $q + 1$, using w satisfying $2 \times w \times$ prime $q + 1$ = the verification value (*mod* the management information);

a primality testing step of testing primality of the calculated prime candidate N; and

an output step of outputting the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined.

31. The prime-calculation computer program of Claim 30 stored in a computer-readable recording medium.

32. The prime-calculation computer program of Claim 30 to be transmitted on a carrier wave.

33. A prime verification method used in a prime verification apparatus that (i) verifies the prime *N* output from a prime calculating apparatus of Claim 1, and (ii) includes an information storage unit storing the management information and the verification value, the prime verification method comprising:

a subtraction step of obtaining a prime subtraction value by subtracting the verification from the prime *N*;

a judgment step of judging whether the obtained prime subtraction value is divisible by the management information; and

a control step of permitting use of the prime *N* when the judgment is affirmative, and prohibiting the use of the prime *N* when the judgment is negative.

34. A prime-verification computer program used on a prime verification apparatus that (i) verifies the prime *N* output from a prime calculating apparatus of Claim 1, and (ii) includes an information storage unit storing the management information and the verification value, the prime verification method comprising:

a subtraction step of obtaining a prime subtraction value by subtracting the verification from the prime *N*;

a judgment step of judging whether the obtained prime subtraction value is divisible by the management information; and

a control step of permitting use of the prime *N* when the judgment is affirmative, and prohibiting the use of the prime *N* when the judgment is negative.

35. The prime-verification computer program of Claim 34 stored in a computer-readable recording medium.

36. The prime-verification computer program of Claim 34 to be transmitted on a carrier wave.

5